

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of)
 (Briefly describe the property to be searched)
 or identify the person by name and address))
 Facebook account of Charles Palmer with ID:)
 100060618555099 (See Attachment A))

Case No. 22-986M(NJ)

Matter No.: 2022R00300**WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS**

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____

(identify the person or describe the property to be searched and give its location):

See Attachment A, over which this Court has jurisdiction pursuant to 18 U.S.C. §§ 2703 and 2711 and Federal Rule of Criminal Procedure 41.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before September 9, 2022 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

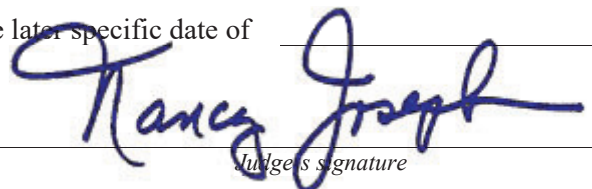
The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to _____

Honorable Nancy Joseph

(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued: 8/26/2022 @ 3:21 p.m.


Judge's signature

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate Judge

Printed name and title

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <div style="display: flex; justify-content: space-between; align-items: flex-end;"> <div style="width: 30%;"> <p>Date: _____</p> </div> <div style="width: 65%;"> <div style="text-align: right; margin-bottom: 10px;"> <p>_____</p> <p><i>Executing officer's signature</i></p> </div> <div style="text-align: right;"> <p>_____</p> <p><i>Printed name and title</i></p> </div> </div> </div>		

ATTACHMENT A

Property to Be Searched

To the extent that the information described in Attachment B is within the possession, custody, or control of Facebook, Facebook is required to disclose to the government the information, for the dates of May 1, 2022, to the present, for the following account:

FACEBOOK NAME	FACEBOOK IDENTIFICATION (UID)
Charles Palmer	100060618555099

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Facebook

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook, including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each user ID listed in Attachment A:

- a. All contact and personal identifying information, including: full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
- b. All activity logs for the account and all other documents showing the user's posts and other Facebook activities;
- c. All photos uploaded by that user ID and all photos uploaded by any user that have that user tagged in them;
- d. All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

- e. All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending “Friend” requests;
- f. All “check ins” and other location information;
- g. All IP logs, including all records of the IP addresses that logged into the account;
- h. All records of the account’s usage of the “Like” feature, including all Facebook posts and all non-Facebook webpages and content that the user has “liked”;
- i. All information about the Facebook pages that the account is or was a “fan” of;
- j. All past and present lists of friends created by the account;
- k. All records of Facebook searches performed by the account;
- l. All information about the user’s access and use of Facebook Marketplace;
- m. The types of service utilized by the user;
- n. The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- o. All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;
- p. All records pertaining to communications between Facebook and any person regarding the user or the user’s Facebook account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(1) and 18 U.S.C. § 2252A(a)(5)(B), since

May 1, 2022, for the user ID identified on Attachment A, information pertaining to the following matters:

- (a) The relevant offense conduct, any preparatory steps taken in furtherance of the criminal scheme, and communications between Brandon Gilmore and others related to the relevant offense conduct of possession, receipt, transportation or distribution of child pornography.
- (b) Evidence indicating how and when the Facebook account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook account owner;
- (c) Evidence indicating the Facebook account owner's state of mind as it relates to the crimes under investigation;
- (d) The identity of the person(s) who created or used the user ID; and
- (e) The identity of the person(s) who communicated with the user ID about matters relating to relevant offense conduct of possession, receipt, transportation or distribution of child pornography.

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
Facebook account of Charles Palmer with ID:
100060618555099 (See Attachment A)

Case No. 22-986M(NJ)
Matter No.: 2022R00300

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, over which this Court has jurisdiction pursuant to 18 U.S.C. §§ 2703 and 2711 and Federal Rule of Criminal Procedure 41.

located in the _____ District of _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2256(8); § 2256 (2);	Possession, receipt or distribution of child pornography; possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct.

The application is based on these facts:
See attached affidavit.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

SA Daniel Gartland, FBI

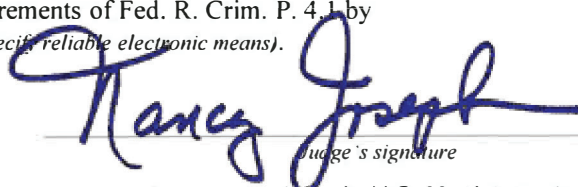
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
_____ telephone _____ (specify reliable electronic means).

Date:

8/26/2022

City and state: Milwaukee, WI



Judge's signature

Hon. Nancy Joseph, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Daniel Gartland, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION, BACKGROUND, TRAINING, AND EXPERIENCE

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been so employed since May 2018. As such, I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request search and arrest warrants. I am currently assigned to the FBI Milwaukee Division and am a member of the Milwaukee Child Exploitation and Human Trafficking Task Force. I am authorized to investigate violent crimes against children, to include the possession, production, and distribution of child sexual abuse material (commonly known as "CSAM").

2. I have received training related to the investigation and enforcement of federal child pornography and child exploitation laws. As a result of this training and my experience, I am familiar with the methods by which electronic devices are used as the means for receiving, transmitting, possessing, and distributing images and videos depicting minors engaged in sexually explicit conduct (hereafter referred to as "child pornography"). I have also received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, electronic device evidence identification, electronic device evidence seizure and processing, and various other criminal laws and procedures.

3. This affidavit is based upon my personal knowledge, my training and experience, and on information reported to me by other federal, state, and local law enforcement officers during the course of their official duties, all of whom I believe to be truthful and reliable. This affidavit is also based upon police reports, official records, citizen witnesses' statements, consent searches,

recorded statements, law enforcement surveillance, surveillance video, social media, court records, telephone records, and public records which I consider to be reliable as set forth herein. The facts of this Affidavit are based upon information obtained from my investigation, as well as information I have received from other law enforcement officers.

4. Based on the investigation to date, I submit that there is probable cause to believe that the information described in Attachment A contains evidence, contraband and/or instrumentalities of violations of 18 U.S.C. § 2252(a)(4)(B) and 18 U.S.C. § 2252A(a)(2)(A), as described in Attachment B.

5. This affidavit is submitted in support of an application for a search warrant for Brandon Gilmore's Facebook account, for evidence of his involvement in the transportation or possession of child pornography, in violation of 18 U.S.C. § 2252A(a)(1), which makes it a crime to transport child pornography, and 18 U.S.C. § 2252A(a)(5)(B), which makes it a crime to possess child pornography, between May 6, 2022, and August 12, 2022.

6. More specifically, I seek authorization to search Facebook's information associated with Brandon Gilmore (DOB XX/XX/1989), who is the user associated with the Facebook account with the following user name and ID number:

FACEBOOK NAME	FACEBOOK IDENTIFICATION (UID)
Charles Palmer	100060618555099

7. The information I seek is stored at premises owned, maintained, controlled, or operated by Facebook, a social networking company headquartered in Menlo Park, California, from at least approximately May 1, 2022, to the present.

8. Because this affidavit is submitted for the limited purpose of obtaining a search warrant, I have not included each and every fact known to me concerning this investigation. I have

attempted to set forth only the facts I believe are pertinent to establishing the necessary foundation for the warrant.

II. DEFINITIONS

1. The following definitions apply to the Affidavit and Attachments A and B to this Affidavit:

a. “Cellular telephone” or “cell phone” means a hand held wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books”; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may include geolocation information indicating where the cell phone was at particular times.

b. “Child Pornography” is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

c. “Computer” is defined pursuant to 18 U.S.C. § 1030(e)(1) as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.”

d. “Computer Server” or “Server,” is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer that hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user’s computer via the Internet. A domain name system (DNS) server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol (IP) address so the computer hosting the web site may be located, and the DNS server provides this function.

e. “Computer hardware” means all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

f. “Computer software” is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is

stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. “Computer-related documentation” consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

h. “Computer passwords, pass phrases and data security devices” consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

i. “Electronic storage devices” includes computers, cellular telephones, tablets, and devices designed specifically to store electronic information (e.g., external hard drives and USB “thumb drives”). Many of these devices also permit users to communicate electronic information through the internet or through the cellular telephone network (e.g., computers, cellular telephones, and tablet devices such as an iPad).

j. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

k. “Internet Service Providers” (ISPs) are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an “e-mail address,” an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider (ISP) over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

l. “An Internet Protocol address” (IP address) is a unique numeric address used by internet-enabled electronic storage devices to access the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every electronic storage device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that electronic storage device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static, that is, long-term IP addresses, while other computers have dynamic that is, frequently changed IP addresses.

m. “Hash Value” refers to the process of using a mathematical function, often called an algorithm, to generate a numerical identifier for data. A hash value can be thought of as a “digital fingerprint” for data. If the data is changed, even very slightly (like the addition or

deletion of a comma or a period), the hash value changes. Therefore, if a file such as a digital photo is a hash value match to a known file, it means that the digital photo is an exact copy of the known file.

n. “Media Access Control” (MAC) address means a hardware identification number that uniquely identifies each device on a network. The equipment that connects a computer to a network is commonly referred to as a network adapter. Most network adapters have a MAC address assigned by the manufacturer of the adapter that is designed to be a unique identifying number. A unique MAC address allows for proper routing of communications on a network. Because the MAC address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.

o. “Minor” means any person under the age of eighteen years. See

18 U.S.C. § 2256(1).

p. The terms “records,” “documents,” and “materials” include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including writings and drawings), photographic form (including prints, negatives, videotapes, motion pictures, and photocopies), mechanical form (including printing and typing) or electrical, electronic or magnetic form (including tape recordings, compact discs, electronic or magnetic storage devices such as hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, smart cards, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

q. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the

same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

r. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

III. PROBABLE CAUSE

1. On May 9, 2022, the National Center for Missing and Endangered Children (NCMEC) received information from Dropbox, Inc. (Dropbox) that suspected Child Sexual Abuse Material (CSAM) was uploaded to the Dropbox account belonging to user Brandon Gilmore. The following user information was provided:

- a. Email address: thememuzickent@gmail.com
- b. Screen/username: Brandon Gilmore

2. Dropbox provided six videos uploaded to the account associated with user Brandon Gilmore. NCMEC provided the information to the Federal Bureau of Investigation for further action. The first video showed a female removing her clothes and touching her vagina. The video then showed an adult male touch her vagina and engaged in vaginal and anal sex with the female. The female appeared to be in the early stages of puberty with minor breast development and some pubic hair. The second video showed adult male engaged in vaginal sex with a minor female. The female appeared to be pre-pubescent, lacking pubic hair and breast development. The third video showed an adult male engaged in oral sex with a minor female. The female wore a blindfold over her eyes. The words, “suck cock cum slut” were written on the blindfold. The female had facial features consistent with a pre-pubescent child. The fourth video showed a close-up view of an adult male engaged in vaginal sex with a pre-pubescent female, lacking pubic hair. The fifth video depicted an adult male laying on a bed while two unclothed females removed his pants and touched

his penis and testicles. The females appeared to be pre-pubescent, lacking breast development and pubic hair. The sixth video showed a female sitting on a chair with her pants pulled down. An adult male then lifted her legs displaying her anus and vagina. The video then showed the male spreading open the minor female's vagina. The female appeared to be pre-pubescent, lacking breast development and pubic hair. The female also wore a t-shirt with a cartoon drawing of a smiling sun. An upload log provided by Dropbox indicated the videos were uploaded on or about May 7, 2022.

3. On June 6, 2022, Dropbox provided information in response to a subpoena requesting user account information and IP addresses associated with the Dropbox user Brandon Gilmore. The information revealed that the account was accessed by IP address 2600:1700:9434:6190:40dd:39d3:ced6:f56e on May 7, 2022.

4. Further investigation determined that the IP address 2600:1700:9434:6190:40dd:39d3:ced6:f56e was assigned to an AT&T account with the following subscriber information:

- i. Account Number: 314010876
- ii. Subscriber Name: Brianna Roeck
- iii. Account Creation: 06/11/2021
- iv. Service Address: 3640 South 87th Street, Milwaukee, WI, 53228

5. A search of law enforcement databases revealed that in June of 2021 Brandon Gilmore (XX/XX/1989) was involved in a vehicular accident in Milwaukee, WI, while driving a black Chevrolet Equinox bearing Wisconsin registration plate ACS-3373 (hereinafter "Equinox"). The registered owner of the Equinox was Brianna Roeck. Gilmore also owns a blue 2004 Chevrolet Impala registered with the state of Wisconsin at the address 3640 South 87th Street, Milwaukee, WI.

6. On July 25, 2022, Special Agents with the Federal Bureau of Investigation (FBI) observed Brianna Roeck arrive at 3640 South 87th Street, Milwaukee, WI, driving the Equinox. Agents observed Gilmore leave the address and return while driving the Equinox. Agents also observed a blue Impala without visible plate parked at the address.

7. An open-source search of Facebook revealed a profile with the name, “Brianna Röck.” The profile includes references to the “Gilmore’s” and includes photos that appear to show Brianna Roeck and Brandon Gilmore together. The profile also contains references to Brynlee Gilmore, a baby born in early-October 2021 and photos of two other female children. Based upon the information in the Facebook profile, I believe Brianna Roeck and Brandon Gilmore are in a relationship.

8. A search of law enforcement databases revealed that Brandon Gilmore is a registered sex offender and resides at the address 3640 South 87th Street, Milwaukee, WI. On July 23, 2013, Gilmore was arrested by the FBI in Minneapolis, MN, for a violation of Title 18 U.S.C. § 2423 (d) and (e) Conspiracy to Facilitate in Transportation of Minors for Prostitution. The arrest was the result of an investigation into Gilmore and two other females for the transportation of a 14-year-old female from Milwaukee, WI to Bloomington, MN for the purpose of engaging in prostitution. Gilmore plead guilty to the charge and was sentenced to 82 months in federal prison and 60 months of supervised release. Gilmore remained on supervision with the United States Probation Office for the Eastern District of Wisconsin as of July 26, 2022, and was due to complete his supervision on August 13, 2024.

9. On July 27, 2022, a search warrant, issued in the United States District Court for the Eastern District of Wisconsin on July 27, 2022, was executed by the FBI at 3640 South 87th Street, Milwaukee, WI. During the search, law enforcement officers seized as evidence an Apple iPhone 13 with serial number: DPQ00N306, (hereinafter, “the Phone”) from the location. Pursuant

to the search warrant, a forensic examination of the phone. The was assigned telephone number 414-708-5314 and had an Apple ID associated with the e-mail address, thememuzickent@gmail.com.

10. The Phone appeared to have an initial power on date of June 26, 2022. The phone included data from dates prior to the initial power on date. Based on my training and experience, I believe the user of the phone obtained a new device on or about June 26, 2022 and synced the Phone with data maintained in on an external cloud-based server.

11. The phone contained several social media accounts and associated conversations. A Facebook profile and Facebook Messenger account on the phone was associated with the username **Charles Palmer** with the **identification number 100060618555099**. A Kik messenger account with a username of “bgillie08” and the e-mail address, Ovathatop01@gmail.com. The Apple wallet for the Phone was associated with “Brandon Gilmore” at the address 4597 North Houston Avenue, Milwaukee, WI. Law enforcement databases indicate that 4597 North Houston Avenue, Milwaukee, WI is the address of Tequila Matthews, mother of Brandon Gilmore.

12. Investigators conducted a review of Kik messenger conversations recovered from the telephone. At least two conversations contained discussions of Child Sexual Abuse Material (CSAM). On July 17, 2022, Kik user “claraoglyta_cb5” (hereinafter, “CB5”) initiated a conversation with the account associated with the phone. CB5 asked “Are you a buyer of cp mega link and video?” CB5 further provided an apparent list of the types of CSAM available. Bgillie08 responded “Samples.” A link to at least one video of suspect CSAM was sent to Bgillie08 and a request for payment was made. On July 25, 2022, Bgillie08 messaged “Samples” to Claraoglyta_cb5, though the message did not appear to be delivered.

13. A Kik conversation between bgillie08 and dirtydaughter101_n1k (hereinafter, “N1K”) occurred from July 17, 2022 to July 25, 2022. The conversation began with N1K sending

links of known or suspected CSAM to Bgillie08 and a request to “Send me the screenshot baby.” Bgillie08 responds with a screenshot of a \$50 payment via an electronic funds transfer application to a user named “Malacia Hyche.” Bgillie08 then messages, “Penetration and cum” and “And anal.” N1K then provided additional videos. Bgillie08 later states, “I’ll send more money when I have all 50 videos u promised for the 30 I sent.” After receiving a series of videos, Bgillie08 states, “That’s not cp. That don’t count.” Further videos and requests for money were sent from N1K until July 19, 2022. On July 25, 2022, the conversation ended with Bgillie08 asking, “Samples?”

14. Investigators conducted a review of the images and videos recovered from the Phone. The phone contained numerous selfie-style images of Brandon Gilmore, including metadata with a location in the area of 3640 South 87th Street, Milwaukee, WI. The phone contained approximately 34 videos of known or suspected CSAM. Five of these videos are further described as follows:

- A close-up video of an infant, approximately less than one year of age, with a white fabric background. The child did not appear to have developed lower teeth. The child’s bare chest was visible in the video. The child appeared to be Caucasian, though hair color and sex of the child could not be determined based upon the view of the camera. An erect adult penis was inserted into the child’s mouth during the video. The video appeared to have been recovered from applications on the Phone.
- A video of a pre-pubescent female, approximately four to eight years of age, laying on her back with her legs held up. The female had short dark brown or black hair and a light skin tone. The child did not have developed breasts or pubic hair. The child’s mannerisms were consistent with a mental handicap. Written on the inner thigh of the child’s left leg is the letter “I”, a drawing of a heart and an illegible word. The female child was completely naked, and her anus and vagina were clearly

visible. There was apparent male ejaculate on the child's legs, vagina and seeping from her anus. A white-skinned adult hand with manicured fingernails pointed to the ejaculate in the child's anus. The video appeared to have been recovered from applications on the Phone.

- A video of a pre-pubescent female, approximately five to nine years of age, visible from the mid-torso down. The child was light skinned. Her face and hair were not visible in the video. The female was wearing a pink and white striped bathing suit with a pink and blue flowers or starfish pattern. The child's bathing suit was pushed to the side and her vagina was partially visible. A white skinned adult male penis had vaginal sex with the child. The adult male's right hand was pressed down on the child's stomach area. The video appeared to have been recovered from applications on the Phone.
- A video of a pre-pubescent female, approximately five to nine years of age, standing in front of a white skinned adult male. The female child is light skinned with short brown hair. The female was wearing a white T-shirt and did not appear to be clothed from the waist down. The female did not appear to have developed breasts. The adult male was wearing a white T-shirt pulled up above his belly button. The adult male has the child perform oral sex on him. The adult male had one hand on the child's shoulder and the other hand manipulated a the zoom on a camera with a remote. The video appeared to have been recovered from applications on the Phone.
- A video of a pre-pubescent female, approximately two to six years of age, lying on a carpeted floor. The child was light skinned. The child did not have pubic hair. Her face and hair were not visible in the video. The child appeared to be wearing a green

T-shirt, pulled up above her chest. The child's vagina was clearly visible in the video. A dark-skinned adult male with an erect penis had anal and vaginal sex with the child before ejaculating on the child's pubic area. The adult male held the child down at various points in the video by gripping the child's waist. The video appeared to have been recovered from applications on the Phone.

15. On July 27, 2022, Brandon Gilmore was interviewed by Special Agents of the FBI in a non-custodial setting at the FBI Milwaukee Field Office. During the interview, Gilmore stated that he had a Dropbox account when he was first released from prison. The account was registered with the e-mail address thememuzickent@gmail.com. Gilmore maintained a few self-developed rap songs on the account and had not used it in several years. Gilmore also used the e-mail address ovathatop01@gmail.com. Gilmore provided the pass code to his phone and stated that he did not have Dropbox on the phone. He further stated that there was not child pornography on his phone. Gilmore stated he "was not concerned about child pornography" and "did not watch child pornography."

IV. FACEBOOK INFORMATION

16. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

17. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state, and

zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

18. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a “Friend Request.” If the recipient of a “Friend Request” accepts the request, then the two users will become “Friends” for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user’s account includes a list of that user’s “Friends” and a “News Feed,” which highlights information about the user’s “Friends,” such as profile changes, upcoming events, and birthdays.

19. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create “lists” of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

20. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post “status” updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming “events,” such as social occasions, by listing the event’s time, location, host, and guest list. In addition, Facebook users can “check in” to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A

particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

21. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

22. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a Chat feature that allows users to send and receive instant messages through Facebook. These chat communications are stored in the chat history for the account. Facebook also has a Video Calling feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

23. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

24. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or

content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become “fans” of particular Facebook pages.

25. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

26. Each Facebook account has an activity log, which is a list of the user’s posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as “liking” a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user’s Facebook page.

27. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs (“blogs”), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

28. The Facebook Gifts feature allows users to send virtual “gifts” to their friends that appear as icons on the recipient’s profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other “pokes,” which are free and simply result in a notification to the recipient that he or she has been “poked” by the sender.

29. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

30. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications (“apps”) on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user’s access or use of that application may appear on the user’s profile page.

31. Some Facebook pages are affiliated with groups of users, rather than one individual user. Membership in the group is monitored and regulated by the administrator or head of the group, who can invite new members and reject or accept requests by users to enter. Facebook can identify all users who are currently registered to a particular group and can identify the administrator and/or creator of the group. Facebook uses the term “Group Contact Info” to describe the contact information for the group’s creator and/or administrator, as well as a PDF of the current status of the group profile page.

32. Facebook uses the term “Neoprint” to describe an expanded view of a given user profile. The “Neoprint” for a given user can include the following information from the user’s profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Facebook user identification numbers; groups and networks of which the user is a member, including the groups’ Facebook group identification numbers; future and past event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Facebook applications.

33. Facebook also retains Internet Protocol (“IP”) logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user’s IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

34. Social networking providers like Facebook typically retain additional information about their users’ accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service

(including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

35. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's “Neoprint,” IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to “tag” their location in posts and

Facebook “friends” to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner’s state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

36. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

IV. INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

37. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment.

V. CONCLUSION

38. Based upon the facts contained within this affidavit, I believe that probable cause exists to search Brandon Gilmore’s Facebook Account for further evidence of his involvement in the possession, receipt, transportation, or distribution of child pornography, in violation of Title 18, United States Code, Sections 2252A(a)(1) and 18 U.S.C. § 2252A(a)(5)(B) between May 1, 2022, and August 16, 2022.

ATTACHMENT A

Property to Be Searched

To the extent that the information described in Attachment B is within the possession, custody, or control of Facebook, Facebook is required to disclose to the government the information, for the dates of May 1, 2022, to the present, for the following account:

FACEBOOK NAME	FACEBOOK IDENTIFICATION (UID)
Charles Palmer	100060618555099

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Facebook

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook, including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each user ID listed in Attachment A:

- a. All contact and personal identifying information, including: full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
- b. All activity logs for the account and all other documents showing the user's posts and other Facebook activities;
- c. All photos uploaded by that user ID and all photos uploaded by any user that have that user tagged in them;
- d. All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

- e. All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending “Friend” requests;
- f. All “check ins” and other location information;
- g. All IP logs, including all records of the IP addresses that logged into the account;
- h. All records of the account’s usage of the “Like” feature, including all Facebook posts and all non-Facebook webpages and content that the user has “liked”;
- i. All information about the Facebook pages that the account is or was a “fan” of;
- j. All past and present lists of friends created by the account;
- k. All records of Facebook searches performed by the account;
- l. All information about the user’s access and use of Facebook Marketplace;
- m. The types of service utilized by the user;
- n. The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- o. All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;
- p. All records pertaining to communications between Facebook and any person regarding the user or the user’s Facebook account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(1) and 18 U.S.C. § 2252A(a)(5)(B), since

May 1, 2022, for the user ID identified on Attachment A, information pertaining to the following matters:

- (a) The relevant offense conduct, any preparatory steps taken in furtherance of the criminal scheme, and communications between Brandon Gilmore and others related to the relevant offense conduct of possession, receipt, transportation or distribution of child pornography.
- (b) Evidence indicating how and when the Facebook account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook account owner;
- (c) Evidence indicating the Facebook account owner's state of mind as it relates to the crimes under investigation;
- (d) The identity of the person(s) who created or used the user ID; and
- (e) The identity of the person(s) who communicated with the user ID about matters relating to relevant offense conduct of possession, receipt, transportation or distribution of child pornography.